REMARKS

Preliminary to the examination of this application, Applicants amend claims 1-48 as shown herein. Additionally, new claims 49-96 are added to more fully claim the disclosed invention. Claims 49-96 are fully supported by the application as filed.

Attached hereto is a marked-up version of the changes made to the claims by the current Amendment. The attached Appendix is captioned "Version With Markings to Show Changes Made".

Applicants submit that claims 1-96 are patentable. Applicants request allowance of the application with these claims. However, if the Examiner feels there is anything further necessary to place this application in condition for allowance, Applicants request the Examiner to telephone Applicants' undersigned representative at the number below.

Respectfully submitted,

By: _____

Christine H. McCarthy
Reg. No. 41,844
Tel. No.: (202) 861-3075
Fax No.: (202) 861-0944

1100 New York Avenue, N.W.
Ninth Floor, East Tower
Washington, D.C. 20005-3918
(202) 861-3651

Enclosure: Appendix

APPENDIX
VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE CLAIMS:

Please amend claims 1-47 as follows:

1. (Amended) An apparatus for selectively encrypting data [sent] for transmission over a network between a server and a client, the apparatus comprising:

means for parsing a first portion of the data from a second portion of the data;

means for encrypting only the first portion of the data; and

means for combining the encrypted first portion of the data with the second portion of the data [which is not encrypted],

wherein the second portion of the data includes more than routing information.

2. (Amended) [An] The apparatus of claim 1, wherein the data [is] includes streaming data.

3. (Amended) [An] The apparatus of claim 1, wherein the first portion of the data includes [is information constituting] payload data [and comprising multimedia data].

4. (Amended) [An] The apparatus of claim 1, wherein the second portion of the data [is non-payload data containing] includes at least one of a header, control data and routing data.

5. (Amended) [An] The apparatus of claim 1, further comprising means for sending the combined first and second portions of the data over the network to the client.

6. (Amended) [An] The apparatus of claim 1, further comprising means for receiving the data from the server before the data is sent over the network to the client.

7. (Amended) [An] The apparatus of claim 1, further comprising means for establishing a data stream between the server and the client.

8. (Amended) [An] The apparatus of claim 1, further comprising key-negotiating means for negotiating an encryption key with the client.

9. (Amended) [An] The apparatus of claim 8, wherein key negotiation [can occur dynamically throughout the process of streaming and encryption] and key exchange occur during transmission of a stream.

10. (Amended) [An] The apparatus of claim 9, wherein encryption by the encrypting means is transparent to the server.

11. (Amended) [An] The apparatus of claim 8, wherein key negotiation can determine the correctness of the result.

12. (Amended) [An] The apparatus of claim 1, further comprising decrypting means installed at the client for decrypting the [combined] first [and second portions] portion of the data.

13. (Amended) [An] The apparatus of claim 1, wherein the parsing means parses the data into different portions based on media format.

14. (Amended) [A] The apparatus of claim 1 wherein the encrypting means encrypts the first portion of the data based on media format.

15. (Amended) [An] The apparatus of claim 1, wherein the apparatus is implemented [as one of] utilizing an application [and] that includes a pluggable core encoding an encryption algorithm for encrypting the first portion of the data, wherein the pluggable core enables the encryption algorithm to be readily changed [plug-in object].

16. (Amended) [A server equipped with the] The apparatus of claim 1, wherein the apparatus in implemented on a encryption bridge.

17. (Amended) A method for selectively encrypting data [composed of] received from a data source, the data including first and second portions which differ from each other in at least [on] one characteristic, the received data to be [being] subsequently sent over a network [between a server and] to a client, the method comprising:

parsing the received data into portions including the first and second portions;

encrypting [only] the first portion of the received data; and

sending the received data including the encrypted first portion and the second portion of the received data over the network to the client.

18. (Amended) [A] The method of claim 17, [further comprising receiving the data from the] wherein the data source is a server.

19. (Amended) [A] The method of claim 17, further comprising determining whether a stream is established between the server and the client.

20. (Amended) [A] The method of claim 15, further comprising negotiating an encryption key with the client.

21. (Amended) [A] The method of claim 20, wherein the received data from the data source is streaming data sent [from the server] during a streaming session and [said step of] the negotiating of the encryption key is carried out [throughout] during the streaming session.

22. (Amended) [A] The method of claim 20, wherein the received data from the data source is streaming data sent during a streaming session, the method further comprising examining the client during the streaming session and terminating [a] the streaming session if [it is found that] the encryption key on the client is invalid.

23. (Amended) [A] The method of claim [17] 20, wherein the encryption key is negotiated with a decryption shim on the client.

24. (Amended) [A] The method of claim 17, further comprising determining whether the received data is streaming data.

25. (Amended) [A] The method of claim 24, further comprising [ignoring] parsing, encypting and sending the data if the data is streaming data and sending the data if the data is not streaming data.

26. (Amended) [A] The method of claim 17, further comprising determining whether a shim is present on the client.

27. (Amended) [A] The method of claim 26, further comprising [deploying] sending a shim to the client if it is determined that the shim is not present on the client.

28. (Amended) [A] The method of claim 17, further comprising determining whether an encryption key on the client is current.

29. (Amended) [A] The method of claim 17, wherein the data includes a payload data portion and at least one of a header, control data and routing data.

30. (Amended) [A] The method of claim 29, wherein the first portion of the data [is] includes the payload data portion.

31. (Amended) [A] The method of claim 17, wherein the data received from the data source for sending to the client is a stream of packets, the method further comprising determining whether a packet is the last packet in a data stream.

32. (Amended) [A] The method of claim 31, further comprising receiving feedback from a decryption shim on the client if it is determined that the packet is not the last packet in the data stream.

33. (Amended) [A] The method of claim 17, further comprising determining whether the client is compromised.

34. (Amended) [A] The method of claim 33, further comprising continuing parsing, encrypting and sending the data into the first and second portions if it is determined that the client is not compromised.

35. (Amended) [A] The method of claim 33, further comprising terminating [a streaming session] the sending to the client if it is determined that the client is compromised.

36. (Amended) A method for decrypting[,] streaming data at a client, the data including [composed of the] first and second portions which differ from each other in at least [on] one characteristic, the data having been [being] sent over a network to the client from an encryption source, the encryption source having encrypted [which encrypts] the first portion of the data, the method comprising:

receiving the data sent over the network [from the encryption source to the client];

parsing the data into portions including the first and second portions;

decrypting [only] the first portion of the data; and

passing the decrypted first portion of the data to a higher level of operations for play in the client.

37. (Amended) [A] The method of claim 36, further comprising prior to the parsing, determining whether the data is an [encrypted] unencrypted stream.

38. (Amended) [A] The method of claim 37, further comprising passing the data to a higher [layers] level of operations without parsing and decrypting when it is determined that the data is an [encrypted] unencrypted stream.

39. (Amended) [A] The method of claim 36, further comprising negotiating a decryption key with the encryption source.

40. (Amended) [A]The method of claim 39, wherein the streaming data is [streaming data] sent from the encryption source during a streaming session and said [step of] negotiating the decryption key is carried out [throughout] during the streaming session.

41. (Amended) [A] The method of claim 39, further comprising [termination of] terminating the [encrypted] stream if the encryption key is invalid.

42. (Amended) [A] The method of claim 36, wherein the first portion of the data [is] includes a payload data portion.

43. (Amended) A method of claim 36, wherein the data is sent from the encryption source over the network as a stream of data packets, the method further comprising determining whether a packet received by the client is a last packet in a data stream.

44. (Amended) [A] The method of claim 43, further comprising sending feedback to the encryption source if it is determined that the packet is not the last packet in the data stream.

45. (Amended) [A] The method of claim 36, further comprising determining whether the client is compromised.

46. (Amended) [A] The method of claim 45, further comprising continuing the parsing, decrypting and passing the data [into the first and second portions] as aforesaid if it is determined that the client is not compromised.

47. (Amended) [A] The method of claim 45, further comprising terminating a streaming session if it is determined that [a packet is a last packet in a data stream or if] the client is compromised.

Claims 48-96 are added as new claims.